REMARKS

By the present response, Applicant has amended claims 1, 3-8, 13 and 15 to further clarify the invention. Claims 1-20, 22 and 23 are pending in this application. Reconsideration and withdrawal of the outstanding rejections and allowance of the present application are respectfully requested in view of the above amendments and the following remarks.

In the Office Action, claims 1-8, 13 and 15 have been rejected under 35 U.S.C. § 112, second paragraph. Claims 9 and 16 have been rejected under 35 U.S.C. § 102(b) as being anticipated by "Shared Secret Recovery in RADIUS" (Friedman). Claim 17 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Friedman in view of U.S. Patent No. 6,538,996 (West et al.). Claim 11 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Friedman in view of U.S. Patent No. 6,088,799 (Morgan et al.).

Claims 1-8 would be allowable if rewritten or amended to overcome the rejections under 35 U.S.C. § 112, second paragraph. Claims 10, 12, 14, 18 and 19 have been objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Claims 13 and 15 would be allowable if rewritten or amended to overcome the rejections under 35 U.S.C. § 112, second paragraph, and if they are rewritten in independent form including all of the limitations of the base claim and any intervening claims. Claims 20 and 22-23 have been allowed.

35 U.S.C. §112 Rejections

Claims 1-8, 13 and 15 have been rejected under 35 U.S.C. § 112 second paragraph. Applicant has amended these claims to further clarify the invention and respectfully requests that these rejections be withdrawn.

Allowable Subject Matter

Applicant thanks the Examiner for allowing claims 20-22 and 23, indicating that claims 1-8 would be allowable if amended to overcome the § 112 rejections, that claims 10-12, 14, 18 and 19 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims, and that claims 13 and 15 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims and if they are amended to overcome the § 112 rejections.

35 U.S.C. § 102 Rejections

Claims 9 and 16 have been rejected under 35 U.S.C. § 102(b) as being anticipated by Friedman. Applicant respectfully traverses these rejections.

Friedman discloses a method that can be used to compromise a RADIUS system that has been subject to poor administration. A Shared Secret is used in the authentication between a RADIUS client and a RADIUS server. While the shared server is never transmitted across the network, it is often used in the user-password hiding process and always in the server's response authentication. Through packet capture and exploitation of the fact that the shared secret is the

only unknown present, the shared secret can be recovered, thus directly compromising the clients and servers themselves rather than the user password used to authenticate against those servers.

Regarding claim 9, Applicant submits that Friedman does not disclose or suggest the limitations in the combination of this claim. The Examiner appears to assert (without specific details) that pages 2 and 3 in Friedman disclose all the limitations in claim 9 of the present application. However, this is not writing an authenticator value for authenticating an access-request message, as recited in the claims of the present application. Friedman discloses authentication between a RADIUS client and RADIUS server.

Moreover, Friedman does not disclose or suggest verifying the access-request message by using the authenticator value of the access-request message when the access-request message is received. Friedman merely discloses performing a MD5 hashing function on a shared secret and an authenticator value to get an intermediate value which is transmitted and the process reversed to yield the original password. Friedman is merely directed to showing that the shared secret can also be recovered during authentication between a RADIUS client and RADIUS server.

Further, Friedman does not disclose or suggest processing the access-message if the access-request message is successfully verified, as recited in the claims of the present application. As has been noted, Friedman is merely directed to showing that a shared secret between a client and server can be recovered.

Moreover, Friedman does not disclose or suggest performing user authentication by decrypting an encrypted user password of the processed access-request message using a temporary authenticator value of the processed access-request message and a shared secret key that is known to each of a message transmitter and a message receiver. As noted at the bottom of column 2 and top of column 3, Friedman is directed to an authentication process between client and server, as opposed to the authentication of the user.

Regarding claim 16, Applicant submits that this claim is dependent on independent claim 9 and, therefore, is patentable at least for the same reasons noted regarding this independent claim.

Accordingly, Applicant submits that Friedman does not disclose or suggest the limitations in the combination of each of claims 9 and 16 of the present application. Applicant respectfully requests that these rejections be withdrawn and that these claims be allowed.

35 U.S.C. § 103 Rejections

Claim 17 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Friedman in view of West et al. Applicant has discussed the deficiencies of West et al. in Applicant's previously filed response, and reassert all arguments submitted in that response. Applicant respectfully traverses these rejections and provides the following additional remarks.

Applicant submits that the limitations in the Office Action rejection of claim 17 do not appear to exactly match the limitations in claim 17 of the present application. In any event,

Applicant submits that none of the cited references disclose or suggest the authenticator value being a message digest created by encrypting a temporary access-request message, as recited in the claims of the present application. Friedman does not disclose or suggest these limitations. Further, as noted in Applicant's previously filed response, the mere disclosure in West et al. of a hash function and MD5 hash function, computing a hash function, or how the hash function is computed do not disclose or suggest these limitations in the claims of the present application.

Moreover, none of the cited references disclose or suggest processing the authenticator value to determine if the access-request message is a valid access-request message or an abnormal access-request message. These limitations are neither disclosed nor suggested in the cited references.

Further, none of the cited references disclose or suggest, performing user authentication if it is determined that the access-request message is a valid access-request message and discarding the access-request message if it is determined that the access-request message is abnormal, as recited in the claims of the present application.

Accordingly, Applicant submits that none of the cited references, taken alone or in any proper combination, disclose suggest or render obvious the limitations in the combination of claim 17 of the present application. Applicant respectfully requests that this rejection be withdrawn and that this claim be allowed.

Claim 11 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Friedman in view of Morgan et al. Applicant respectfully traverses this rejection and submits that this claim is dependent on independent claim 9 and, therefore, is patentable at least for the same reasons noted previously regarding this independent claim. Applicant submits that Morgan et al. does not overcome the substantial defects noted previously regarding Friedman.

Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose suggest or render obvious the limitations in the combination of claim 11 of the present application. Applicant respectfully requests that these rejections be withdrawn and that these claims be allowed.

CONCLUSION

In view of the foregoing amendment and remarks, Applicant submits that claims 1-20, 22 and 23 are now in condition for allowance. Accordingly, early allowance of such claims is respectfully requested. If the Examiner believes that any additional changes would place the application in better condition for allowance, the Examiner is invited to contact the undersigned attorney, Frederick D. Bailey, at the telephone number listed below.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this, concurrent and future replies, including extension of time fees, to Deposit Account 16-0607 and please credit any excess fees to such deposit account.

Respectfully submitted,
FLESHNER & KIM, LLP

Daniel Y.J. Kim
Registration No. 36,186
Frederick D. Bailey
Registration No. 42,282

P.O. Box 221200
Chantilly, Virginia 20153-1200
(703) 766-3701 DYK/FDB:tlg
Date: November 21, 2006
\\Fk4\Documents\2000\2000-122\107574.doc
Please direct all correspondence to Customer Number 34610